Claims 9, 15, 17, and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Son in view of Fruehauf and Pinder (US 6,105,134).

Discussion of Son and Fruehauf

Son discloses a system for secure distribution of video on-demand programming. In one embodiment, a video program is encrypted 602 by a video on-demand source 402 to generate an encrypted program in a first encrypted form. The encrypted program is transported 604 via a primary distribution network from the video on-demand source 402 to a remote server 404 within a distribution center 106. A key to decrypt the encrypted program may also be transported from the source 402 to the server 404. The encrypted program is then stored 606 in the remote server 404. The key may be a public key of a public key encryption system. When the remote server 404 receives 608 a request for transmission of the video program from a subscriber station 110, the remote server 404 responds by multiplexing 610 the encrypted program in the first encrypted form (and the key if necessary) with other signals to generate a multiplexed signal. The multiplexed signal is then distributed 612 via the secondary distribution network 108 to subscriber station 110. At the subscriber station 110, the multiplexed signal is demultiplexed 614 to isolate the encrypted program in the first encrypted form (and the key if necessary), and the encrypted program is decrypted 616 to generate the unencrypted video program (Col. 5, lines 5-50).

The goal of Son is to provide a video on-demand system with increased security at the remote server 404 (Col. 1, lines 28-30).

In contrast, the goal of the present invention is to share conditional access data among a number of conditional access providers, thereby enabling interoperability among different terminals which require the conditional access data in different formats. With Applicants' invention, the conditional access data is provided in a first format which is compatible with a first user terminal and also in a second format which is compatible with a second user terminal, thereby enabling different terminals which require conditional access data in different formats to decrypt the encrypted data service. This aspect of the present invention is set forth in paragraph (c) of claim 1.

In contrast, Son provides conditional access data (the encryption key) to all user terminals in a single format. Son does indicate that the encryption key may be transmitted from the source to the server "while encrypted in a second encrypted form" (Col. 5, lines 29-31). However, the "second encrypted form" is merely an encryption format for the key that is different than the encryption format (i.e. the "first encrypted form") used for the encrypted program (Col. 5, lines 6-8). Son does not disclose providing a plurality of encryption formats for the key itself, as apparently assumed by the Examiner.

Further, Son discloses only one conditional access provider (CAP), the video on-demand source 402. The server 404 of Son is not a secondary CAP, as is apparently assumed by the Examiner. In the embodiment described in column 5 of Son referenced by the Examiner, the server 404 does not provide second conditional access data in response to the first conditional access data, as claimed by Applicants. Instead, the server 404 of Son merely acts as a pass through for the encrypted video program and encryption key (Col. 5, lines 4-5). In other described embodiments of Son, the server 404 may decrypt the encrypted program and re-encrypt it in a second form before transmitting it to the subscriber station 110. However, in this embodiment of Son, only the second encrypted form of the video program and the second key are sent to the subscriber station 110.

In contrast, with Applicants' claimed invention, a data stream comprising the at least one encrypted data service and first and second conditional access data are provided to the user terminals, including a first user terminal that is compatible with the first conditional access data and a second user terminal that is compatible with the second conditional access data.

Son does not disclose or remotely suggest providing conditional access data to user terminals in two different formats to enable different types of user terminals to decrypt the same encrypted data, as provided by Applicants' claimed invention.

Son describes a point-to-point video on-demand system. Therefore, the encrypted video of Son is sent to a particular subscriber unit together with the decryption key needed to decrypt the encrypted video. In contrast, Applicants' claimed invention is designed for use, for example, in a television broadcast environment where different subscribers may have different types of user terminals which have different requirements for conditional access data (Applicants' specification, page 1, lines 10-13). To enable the different types of subscriber terminals to co-exist in the same broadcast system, the present invention provides conditional access data in a first format for encrypting at least one data service during a plurality of successive crypto-periods and time data for identifying the successive crypto-periods from a primary CAP to a secondary CAP. The secondary CAP is responsive to the first conditional access data and time data and provides second conditional access data in a different, second format for the successive crypto-periods. A data stream comprising the at least one encrypted data service and the first and second conditional access data is provided to user terminals, including at least a first user terminal that is compatible with the first conditional access data and a second user terminal that is compatible with the second conditional access data.

Son does not address the problem of different types of user terminals in a broadcast system that require conditional access data in different formats, which is solved by Applicants' invention.

The Examiner has acknowledged that Son does not disclose providing time data for identifying successive crypto-periods as claimed by Applicants. The Examiner indicates that Fruehauf discloses Applicants' claimed time data. Fruehauf does disclose first and second timing elements, and first and second key storage units containing a plurality of keys in a predetermined order for selection of keys depending on respective key times, wherein the key times occur periodically according to the first and second timing elements (Col. 1, lines 40-45). Therefore, the timing elements of Fruehauf are used to determine which keys are used at which times, and not to identify successive crypto-periods as claimed by Applicants.

Further, Fruehauf does not cure the deficiencies of Son discussed above. Thus, the proposed combination of Son and Fruehauf does not render Applicants' claims obvious.

In view of the above, Applicants respectfully submit that the present invention would not have been obvious to one skilled in the art in view of Son in combination with Fruehauf or any of the other references of record.

In light of the foregoing, withdrawal of the rejections under 35 U.S.C. § 103(a) is respectfully requested.

Further remarks regarding the asserted relationship between Applicants' claims and the prior art are not deemed necessary, in view of the above discussion. Applicants' silence as to any of the Examiner's comments is not indicative of an acquiescence to the stated grounds of rejection.

Conclusion

The Examiner is respectfully requested to reconsider this application, allow each of the presently pending claims, and to pass this application on to an early issue. If there are any remaining issues that need to be addressed in order to place this application into condition for allowance, the Examiner is requested to telephone Applicants' undersigned attorney.

Respectfully submitted,

Douglas M. McAllister
Attorney for Applicant(s)
Law Office of Barry R. Lipsitz
Registration No. 37,886
755 Main Street
Monroe, CT 06468
(203) 459-0200

**ATTORNEY DOCKET NO.: GIC-599**
Date: January 5, 2004